CallScripter

revolutionising your customer communications

Using CIM Systems for Regulatory Compliance

White Paper

Payment Card Industry (PCI) Data Security Standard

Introduction 3
What is PCI? 3
The PCI security standards council 3
Merchant or service provider? 4
Levels of Classification 4
Service Provider Levels 4
Third Party Service Providers 4
Stages of Compliance 5
Build and maintain a secure network 6
Protect Cardholder Data 6
Maintain a Vulnerability Management Program 8
Implement Strong Access Control Measures 8
Regularly Maintain and Test Networks 9
Maintain an Information Security Policy 9
Compensation Controls 10
How CIM systems can help 10
Encryption 11
Removing fields once transaction is complete 13
Permanent removal of data 13
Payment Gateways 14
Payment Gateway providers 15
CIM integration with Telephony Systems 15
Pausing call recordings from within a script 16
Stop credit card details from entering the contact centre workspace 16
Conclusion 18
The author 19
The company 19

Introduction

The list of rules and regulations covering contact centre operations seems to be continually growing, with potentially large fines for any breaches that occur. Scripting has a major part to play in ensuring that your agents not only act the right way and say the 'right thing', but also allows management to produce compliance reports that demonstrate that adherence is being achieved.

Retaining customers' personal financial details safely and securely is an onerous task. The major credit card companies have become so concerned about credit card theft that they have produced an international standard (The Payment Card Industry Data Security Standard) that all organisations that handle credit card information must implement. This standard is complex (a 75 page requirements document and numerous supporting documents), and implementing it within the contact centre environment is a major project for any business.

Whilst the Payment Card Industry (PCI) specifications are complex, Customer Interaction Management (CIM) systems can be used to help meet vital parts of these requirements. This document presents an overview of the PCI standard and how modern CIM systems can be used to help achieve compliance.

What is PCI?

Back in 2006 the five major credit card payment brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc) launched the Payment Card Industry Security Standards Council. The council's role is to develop and maintain standards for all aspects of handling credit card information.

The PCI security standards council

The standards published by the council cover everything from the point of entry of credit card data into a system, to how the data is processed, through secure payment applications. The rules apply to merchants, processors, financial institutions, and any other organisations that store, process, and transmit cardholder data.

The council website can be viewed at: https://www.pcisecuritystandards.org/

The two main standards are the Payment Card Industry Data Security Standard (PCI DSS) and the Payment Application Data Security Standard (PA-DSS).
PCI DSS 2.0 and PA-DSS Version 2.0 were released in October 2010 and came into effect on 1st January 2011.

Companies that handle credit card information, be it in person, over the telephone or via the Internet, need to comply with PCI DSS 2.0. Manufacturers of devices that read credit cards or authorise payments (web payment gateways for example) must comply with PA-DSS Version 2.0.
It should be noted that whilst the council publishes the PCI Security Standard, it does not validate or enforce an organisations compliance with its standards (nor does it impose penalties for non-compliance). These areas are governed by the payment brands and their partners.

One area where the council does get involved in is the authorisation of companies to perform compliance audits. These companies are known as Qualified Security Assessors (QSA's). Additionally, the council maintains a list of Approved Scanning Vendors (ASV's) – these are companies that can perform penetration tests on your company's network to verify that it cannot be easily hacked remotely by data thieves.

Merchant or service provider?

The first step down the route to PCI compliance is to determine whether your organisation is classified as a Merchant or a Service Provider.
Merchants only process/store credit card information on behalf of their own company (i.e. a contact centre department within a large business)
Service Providers process/store credit card information for other companies (i.e. a contact centre taking calls on behalf of multiple clients)
Levels of Classification
Merchant and Service Providers are further classified depending upon the number of credit card transactions they process per annum.

Levels of Classification

Merchant and Service Providers are further classified depending upon the number of credit card transactions they process per annum.

Level	Type of Business	Actions Required
1	• Any merchant processing over 6 million transactions a year • Any compromised merchant	• Annual onsite security assessment • Quarterly network scan
2	• Any merchant processing 1 to 6 million transactions a year	• Annual Self Assessment Questionnaire • Quarterly network scan
3	• Any merchant processing 20,000 to 1 million transactions a year	• Annual Self Assessment Questionnaire • Quarterly network scan
4	• Any merchant processing fewer than 20,000 transactions a year	• Annual Self Assessment Questionnaire • Quarterly network scan

Service Provider Levels

Level	Type of Business	Actions Required
1	• Any service provider that stores, processes and/or transmits more than 300,000 transactions annually.	• Annual onsite security assessment • Quarterly network scan
2	• Any service provider that stores, processes and/or transmits less than 300,000 transactions annually.	• Annual Self Assessment Questionnaire • Quarterly network scan

Third Party Service Providers

The Data Security Standard (PCI DSS) states:

- Third Parties/Outsourcing

For service providers required to undergo an annual onsite assessment, compliance validation must be performed on all system components in the cardholder data environment.
A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers,

firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.
For those entities that outsource storage, processing, or transmission of cardholder data to third-party service providers, the Report on Compliance (ROC) must document the role of each service provider, clearly identifying which requirements apply to the assessed entity and which apply to the service provider.
There are two options for third-party service providers to validate compliance:

1. They can undergo a PCI DSS assessment on their own and provide evidence to their customers to demonstrate their compliance; or
2. If they do not undergo their own PCI DSS assessment, they will need to have their services reviewed during the course of each of their customers' PCI DSS assessments.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data.

Stages of Compliance

Complying fully with PCI DSS is a 5 step process.

1 Non-Compliant

- No contact between merchant & acquirer
- Merchant either unwilling or unable to progress

2 Preparing

- Contacted by acquirer
- Gap analysis in progress

3 Committed

- Has a Qualified Security Assessor (QSA) or an agreed Independent Assessment
- Gap analysis complete and preparing remediation plan/seeking budget
- Performs network scans using an Approved Scanning Vendor (ASV)

4 In Progress

- Has QSA or agreed Independent Assessment
- Completed gap analysis
- Action plan and remediation plan in place Indication of final audit date
- Passes quarterly network scans using an ASV

5 Compliant

- Internal Audit Completed and passed (Level 1)
- Successfully completed SAQ (Level 2-3-4)
- Passes quarterly network scans using an ASV

The 12 Requirements of PCI DSS

The Data Security Standard is the core document issued by the council. It defines requirements and processes that companies must meet in order to ensure that credit card account data is always secure. It comprises 12 key requirements.

Whilst the majority of the requirements relate to IT network security and management processes, one area where Customer Interaction Management systems (CIM) can readily help is with the 'protect cardholder data' sections of the standard.

Before we discuss in detail where CIM can help, let's take a quick look at all 12 requirements to get a broad understanding of what they mean.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	1.	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open public networks
Maintain a Vulnerability Management Program	5.	Use and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know
	8.	Assign a unique ID to each person with computer access
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

Build and maintain a secure network

1. Install and maintain a firewall configuration to protect cardholder data

2. Do not use vendor-supplied defaults for system passwords and other security parameters

All systems must be protected from unauthorised access and firewalls are a key protection device for any computer network. These two sections of the Data Security Standard specify the minimum requirements for configuration of a company's Local Area Network (LAN).

Interesting Note:
When using laptop computers with 3G telephony connections and connecting to the office network, there is a possibility to bypass the firewall and thus allow hackers to gain unrestricted access into the company's systems.

Protect Cardholder Data

3. Protect stored cardholder data

4. Encrypt transmission of cardholder data across open public networks

If someone does manage to gain unauthorised access to credit card information, then it is important that the data they find is stored in such a way as to be virtually unusable. This is achieved by ensuring that the data is not stored as a plain number, but is modified or encrypted so that is cannot be accessed without a cryptographic key. Additionally, keeping the amount of credit card information stored to an absolute minimum is of paramount importance.

The PCI standard splits credit card data down into two distinct types. Cardholder data, which includes the 16 digit account number on the front of a credit card (PAN), and sensitive authentication data which includes the 3 digit number on the signature strip on

the back of a card (CVV2). Whilst it is permissible to store cardholder data once it has been used to authorise a payment, the data must be protected (usually by encryption). Sensitive authentication data on the other hand, must be destroyed as soon as authorisation has been received.

The table below shows which items of credit card data belong to each data type.
Requirement 3.2: Do not store sensitive authentication data after authorisation (even if encrypted).

Data Element		Storage Permitted	Protection Required
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	Yes
	Service Code	Yes	Yes
	Expiration Date	Yes	Yes
Sensitive Authentication Data	Full Magnetic Stripe Data	No	N/A
	CAV2/CVC2/CVV2/CID	No	N/A
	PIN/PIN Block	No	N/A

These rules about protecting stored cardholder data have a major impact on most organisations as they have to determine all the places where credit card data may inadvertently be stored. For example,

- Database tables
- Call recordings – including network cloud
- Emails – including the 'sent' box of back office staff
- Backup files and offsite storage
- Computer event logs

For further clarification on rule 3.2,

Conversation with Neira Jones; head of Barclaycard PCI compliance division.

- Data storage should be kept to a minimum at all times (if you no longer need any of the card information you should delete it)
- The 16 digit PAN can be stored for as long as required ensuring that it is encrypted with strong encryption
- The 3 or 4 digit CV2 number can be stored using strong encryption until the payment has been authorised – at which point it must be deleted.

DO NOT STORE SENSITIVE AUTHENTICATION DATA POST AUTHORISATION

As far as third party call centres are concerned, where an encrypted email or secure ftp file is sent to the client for subsequent batch processing, Barclaycard would insist that the three digit CVV2 is deleted from call centre records as soon as the encrypted file is sent to the client.

For best practice, once the credit card information has been sent out by the call centre they should:

- Scrub the CVV2 from the database (and any encrypted emails it has got into)
- Either scrub or mask the 16 digit PAN (to a maximum of 123456******1234)

Requirement 4 of the PCI DSS concerns ensuring that any credit card data sent over computer networks, including the company LAN, are encrypted at all times. One of the biggest risks identified is that of badly configured wireless networks where an intruder could gain access via a Wi-Fi connection to steal credit card data.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs

6. Develop and maintain secure systems and applications

Malicious software, commonly referred to as “malware” – including viruses, worms and Trojans – entering the network during many business approved activities including employee email and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know

8. Assign a unique ID to each person with computer access

9. Restrict physical access to cardholder data

To ensure critical data can only be accessed by authorised personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

“Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by and can be traced to known authorised users.

Physical access to systems that store cardholder data must be appropriately restricted to ensure that the storage devices themselves cannot be copied or stolen.

Requirement 9 details how company staff (onsite personnel) and visitors must be treated in order that their opportunity to access card holder data is minimised.
Interesting Note: Password protected screensavers must kick in after 15 minutes Login passwords must be ‘complex’ and change at least every 90 days Visitor badges must be worn

Regularly Maintain and Test Networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

Logging mechanisms and the ability to track user's activities are critical in preventing, detecting, or minimising the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting and analysis when something goes wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. Systems components, processes and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

Interesting Note:

- Buy a Wireless analyser to look for rogue devices
- Install 'File Integrity Monitoring' software 11.2.2
- Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).

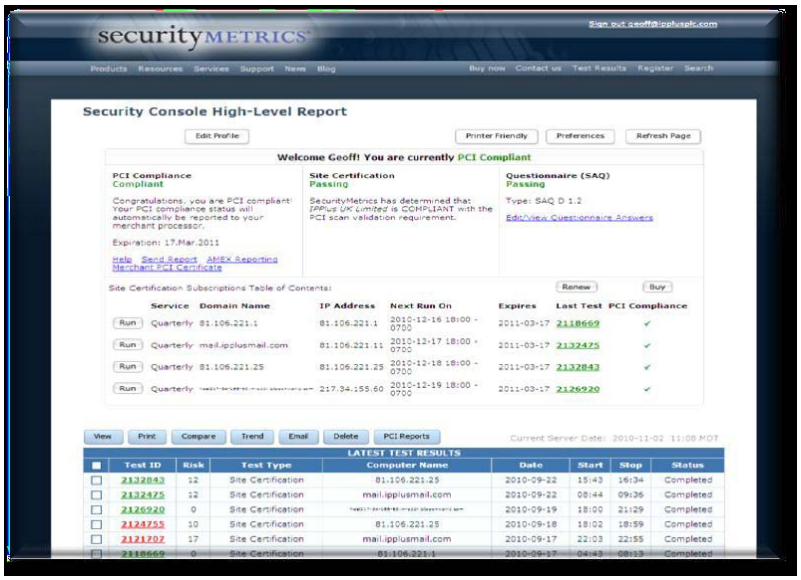

Figure 1 - Results of am ASV quarterly scan

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

A strong security policy sets the security tone for the whole company and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

Interesting Note:

- Make staff aware that they should not copy sensitive data when connected via VPN
- Update your IT Policy document to include an ‘Incident Response Plan’

Compensation Controls

With 12 major requirements splitting down into over 220 sub-requirements, what happens if you cannot meet one of the exacting criteria? To overcome this problem the PCI DSS allows for the creation of compensation controls. For a compensating control to be valid, it must:

Meet the intent and rigour of the original PCI DSS requirement;

1. Provide a similar level of defence as the original PCI DSS requirement;
2. Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements) and
3. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

So, compensating controls are definitely not an easy option as they require systems to be put in place that are just as strict, if not stricter than, the sub requirement they replace.

Note:

- Visa insists that all compensating controls must be approved by an external QSA regardless of the company’s merchant or service provider level.

How CIM systems can help

Customer Interaction Management systems can play a major role in helping a contact centre based operation within a company achieve PCI compliance. Requirements 3 and 4 of the PCI DSS (dealing with protecting cardholder data) lend themselves to CIM based solutions, particularly in the areas of:-

- Encryption
- Removing fields once a transaction is complete
- Payment Gateways
- Archiving of data

During normal operations, your contact centre agents may take credit card information over the phone. The agent will ask for the card details and enter them into a series of fields within the CIM application before they are sent off for processing. This, of course, means that the agent hears the credit card number and types it into the system. Later on we will discuss how CIM can be used to bypass this part of the procedure so that the agent never hears the credit card information, but is still able to converse with the caller at all times – thereby ensuring that the quality of the customer experience is not compromised.

Typically, a modern CIM system runs as a thin client application. This means that the all data and processing work is carried out on a central server that passes script information and customer data across the local area network (LAN) to the agent desktop. Typically the agent application runs within a web browser and it is a simple matter to ensure that the data connection between the server and the desktop is a secure https connection.

Regardless of how the credit card data gets entered into the system, once there it needs to be protected (PCI DSS Requirement 3.4 Render PAN unreadable anywhere it is stored). This may be achieved through using the CIM environment to encrypt the data before it is stored.

Encryption

Encryption is vital to ensure that any stored data (typically the 16 digit PAN on the front of the credit card) is not readily readable by anyone accessing the database. Additionally, reports generated by the CIM system that are sent to a client (typically by email or ftp) must also be encrypted.

The CIM software should support field encryption. Within the CIM script designed, it is simply a matter of identifying fields that could possibly contain sensitive information and then marking them for encryption. The system will then automatically encrypt the field using a master public cryptography key.

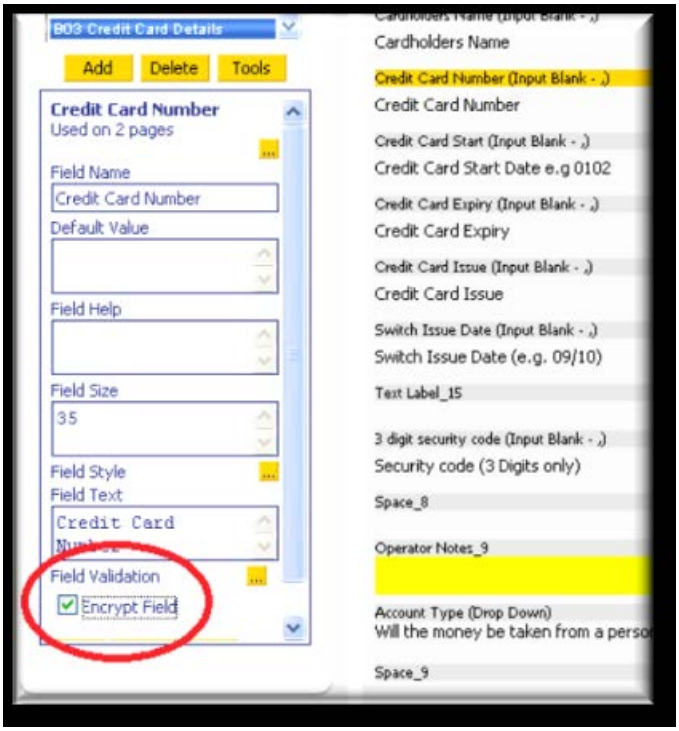

Figure 2 - Setting a credit card field to be encrypted

Cardholder data entered by the contact centre agent into the CIM software is sent via a secure intranet connection to the associated server where it is encrypted using the master public cryptography key before being stored within the database.

Administrative staff, reporting desk personnel, managers and supervisors viewing the data via the CIM system management interfaces will be unable to view the encrypted values, rather they will see a field token telling them that the data is encrypted.

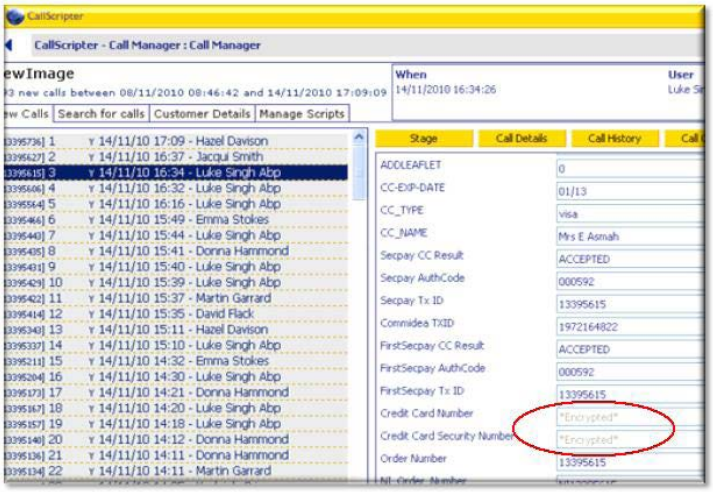

Figure 3 - Encrypted data is not visible to contact centre staff

To retrieve the encrypted data from the CIM system and send it on to the final recipient another public encryption key is used, this one specifically created by the people that are going to be performing the credit card authorisation process. This group generates a public/private cryptography key pair and sends the public part of the key to the contact centre where it is then associated with a credit card report. When the report runs, the encrypted data within the CIM system database is decrypted 'on the fly' using the master private cryptography key known by the system and re-encrypted using the report specific public cryptography key. The report is then sent to the credit card authorisation group who use their private report key to retrieve the data and process it.

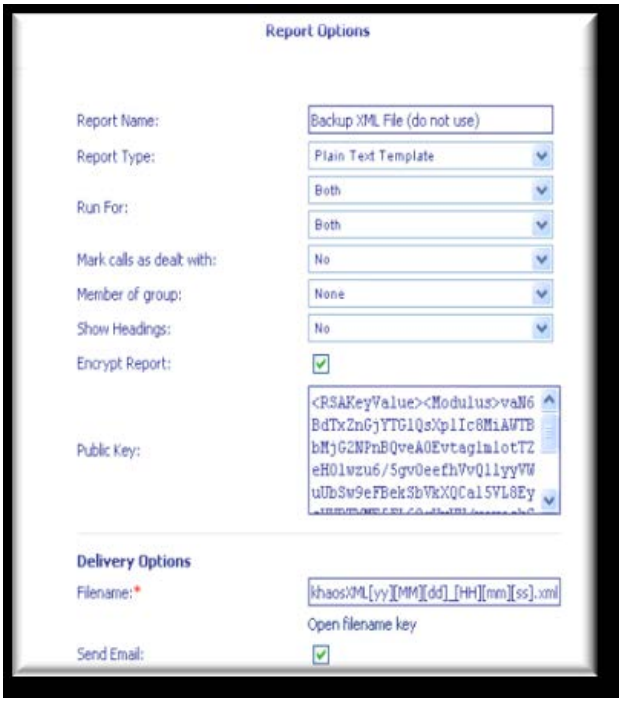

Figure 4 - Reporting systems use a public encryption key

Removing fields once transaction is complete

Ideally an individual encrypted report should be sent as part of each CIM script run. The advantage of this approach is that once the report has been sent, the associated encrypted data still held within the CIM system database can be deleted (thereby complying with PCI requirement 3.2) and ensuring that no sensitive cardholder data is stored (even encrypted) post authorisation.

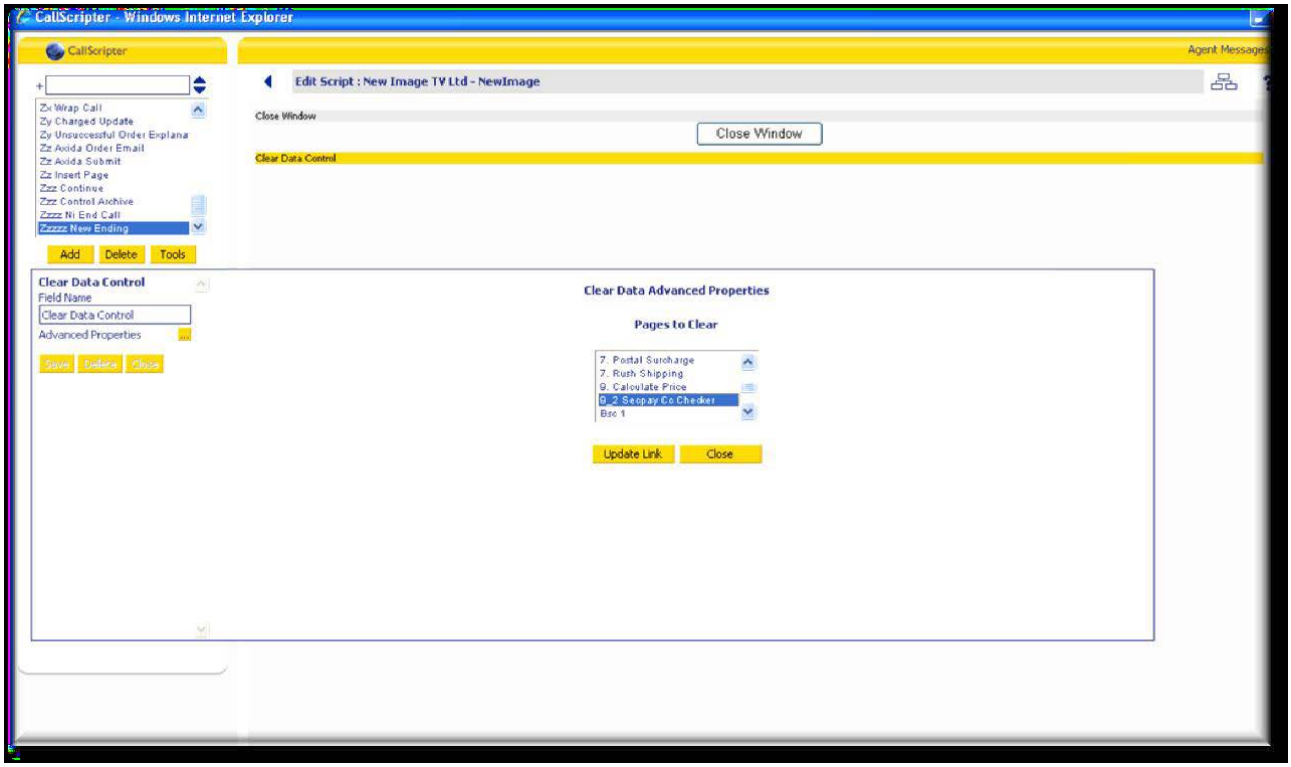

Figure 5 - The CIM system deleting fields once the encrypted credit card data report has been sent

If a batch processing approach to credit card authorisation is being used (for example sending a daily report to a fulfilment house that also processes the credit card payment) then the CIM system should have the ability to automatically block delete the encrypted fields within the CIM database once the batch report has been sent.

Permanent removal of data

PCI requirement 3.1 instructs that all cardholder data storage must be kept to a minimum by implementing data retention and disposal processes. It is therefore important to ensure that the CIM system has the ability to regularly clean out its database, removing any encrypted PAN fields that are no longer needed.

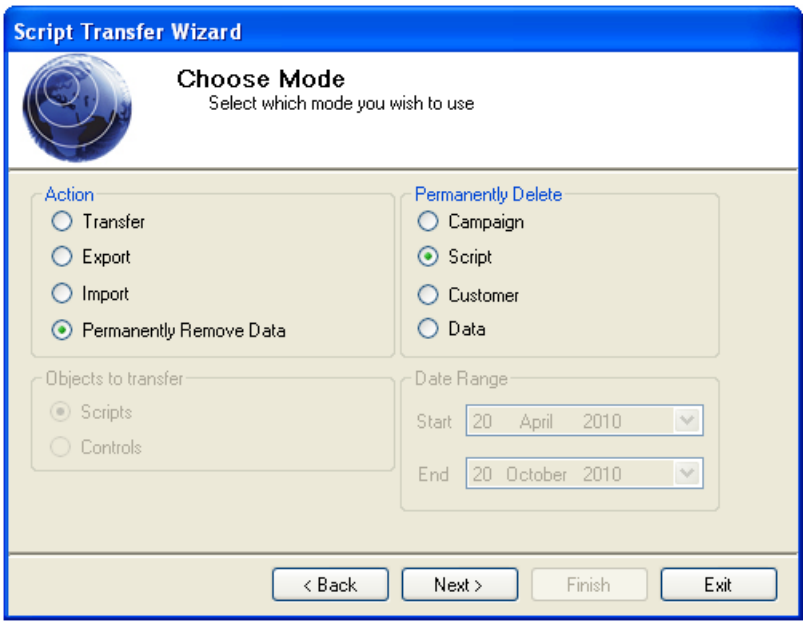

Figure 6 – tool to permanently remove data from the CIM database

Payment Gateways

Whilst temporarily storing encrypted credit card data within the CIM system is one option, it would be preferable to remove the storage need altogether. This can be achieved by using payment gateways.

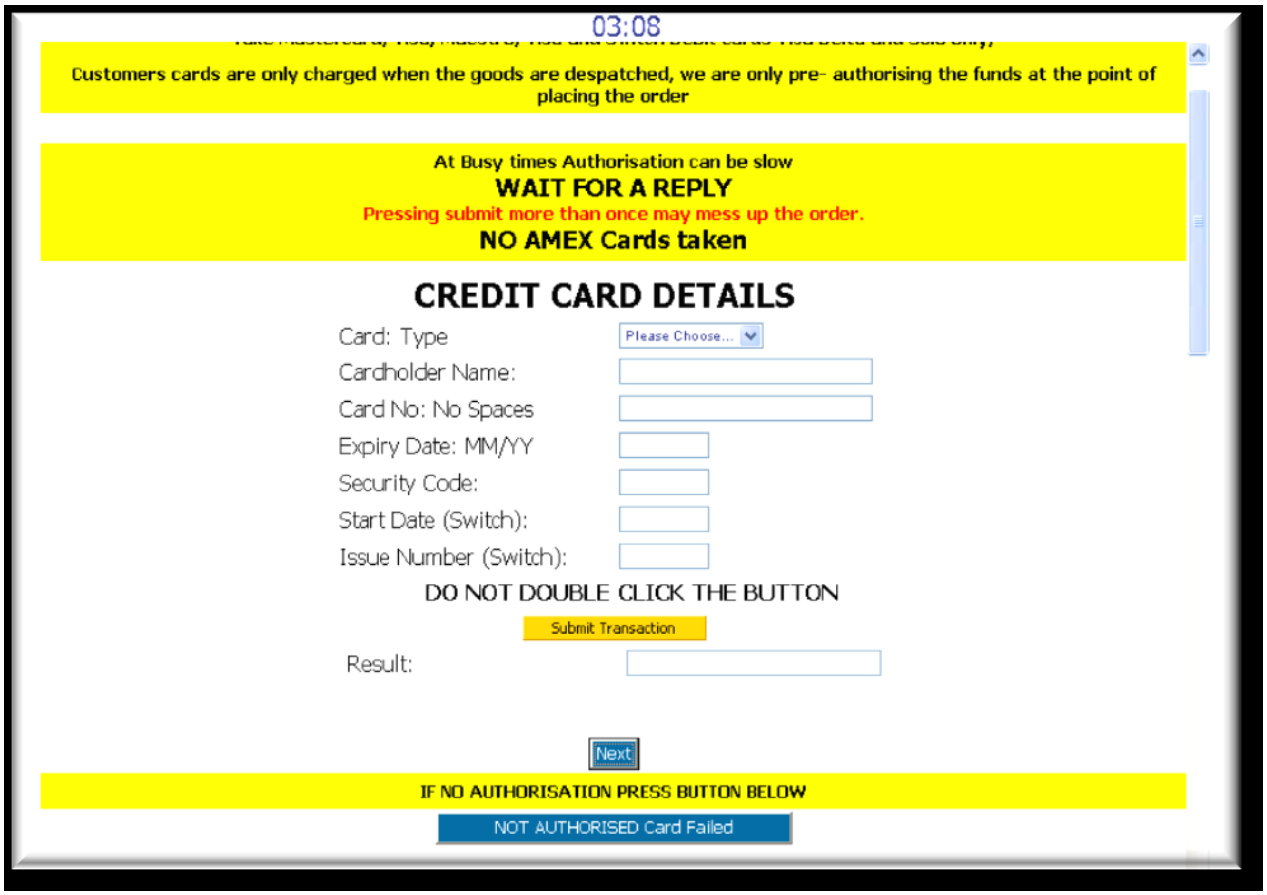

Figure 7 - A payment gateway embedded within a CIM script

A payment gateway is effectively a miniature web page that sits within the CIM script (usually embedded within an I-frame). The payment gateway contains all the necessary fields to take the credit card details, but when completed the information is not stored within the CIM database, rather it is sent directly to a payment gateway provided (a company that verifies the card details and processes the payment on behalf of the credit card company) via a secure internet connection. The payment gateway provider processes the card and returns a transaction authorisation code to the CIM system and it is this authorisation code that is stored within the CIM database as a record of the transaction taking place.

Payment Gateway providers

A payment gateway is an application service provider e-commerce interface that authorises payments for businesses via a secure internet connection. It is the equivalent of a physical point of sale terminal located within the premises. Payment gateways protect credit card details by encrypting sensitive information to ensure that information is passed securely between the customer and the merchant and also between merchant and the payment processor.

Commonly used Payment Gateway providers within the CIM contact centre environment
Bucks.Net (specialist public & charity sectors)
Commidea
DataCash
Flo2Cash (New Zealand)
HSBC
IP Payments (Australia)
NetBanx
Rapidata (specialist charity sector)
Raven
RealCredit
RealEx
SagePay (formally Protx)
SECPay (PayPoint.net)
SecureTrading

CIM integration with Telephony Systems

CIM software has the ability to interact with the contact centre telephony switch through a system called Computer Telephony Integration (CTI). This system is commonly used to associate an incoming phone number with a specific CIM script, causing it to 'screen pop' as the call is put through to the contact centre agent. (For example, the caller dialled 0844 123 123 and this is associated with a new product sales script. As the call is put through to the contact centre agent, their computer screen launches the 'new product sales script' displaying the opening greeting "thank you for calling the new product sales line, how can I help you today?"). Outbound call campaigns are treated in the same way, with the contact centre agent experiencing a screen pop as the outbound call is placed.

All contact centres need to record calls and this causes an issue for PCI compliance as sensitive credit card information could be stored within the call recording sound files. The option to simply not record calls that may contain credit card information is usually a non-starter; fortunately several CIM based solutions are available to help solve this problem.

Pausing call recordings from within a script

When the contact centre agent reaches the part of the call where credit card information needs to be taken, a command is sent from the CIM system to the telephony switch via the CTI link requesting that any call recording in progress is paused. The contact centre agent then takes all the relevant details and once complete a second command is sent from the CIM system instructing the telephony switch to resume the call recording.
Pausing the call recording during the section of the call where credit card information is given is a good solution as it removes the requirement to delete the CVV2 information from the encrypted recording file once the payment has been authorised.

Stop credit card details from entering the contact centre workspace

Pausing the call recording and using payment gateways to stop credit card information entering the CIM system is all well and good, but this still leaves the contact centre open to other PCI compliance requirements. (For example, how do you ensure that the contact centre agents are not writing down credit card numbers and taking them home!).
The best solution would be to use a system where credit card information never enters the contact centre – in other words, making sure that the contact centre agent neither hears or sees the credit card number (PAN) or CVV2.

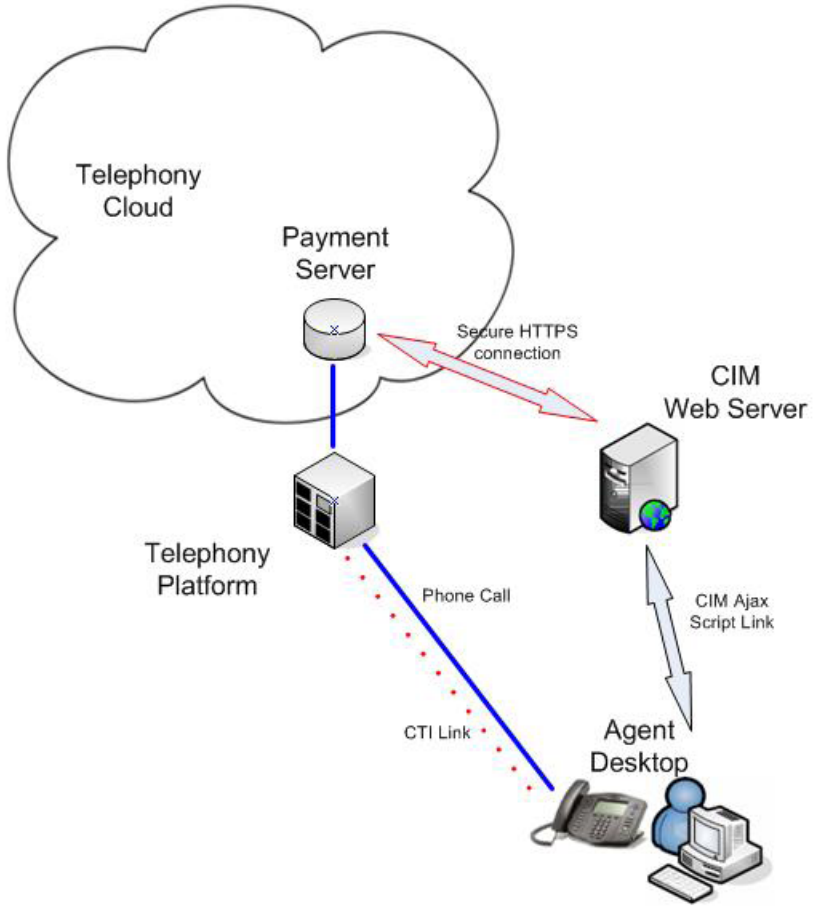

Figure 8 - No credit card details need to enter the contact centre

Various commercial systems are available that completely remove the necessity for contact centre agents to take the credit card details from the caller. These systems work

by asking the caller to input the credit card details by pressing buttons on their telephone keypad rather than speak the credit card number out loud.

The process typically follows the following route. The contact centre agent works with the caller until the credit card payment page is reached within the CIM script. The contact centre agent asks the caller for the name on the front of the credit card and enters this into a field within the script.
At this point the contact centre agent pushes a button on the script page that sends a signal to the telephony platform instructing it to go into 'listening mode' and start intercepting numbers entered by the caller on their keypad. (Using a system called DTMF tones).

The contact centre agent asks the caller to enter the 16 digit credit card number (PAN) using their telephone keypad and each entered digit is captured by the telephony system and sent to the payment server. Additionally the various beeps (DTMF tones) produced by the callers telephone keypad as the credit card number is entered are suppressed by the telephony platform so that they are neither heard by the contact centre agent or present on call recordings. As each individual number is entered by the caller a signal is sent to the CIM system so that is can display a series of asterisks in the CIM script credit card number field thereby showing the progress being made.

The above process is repeated for the 3 digit CVV2 security number on the back of the card.

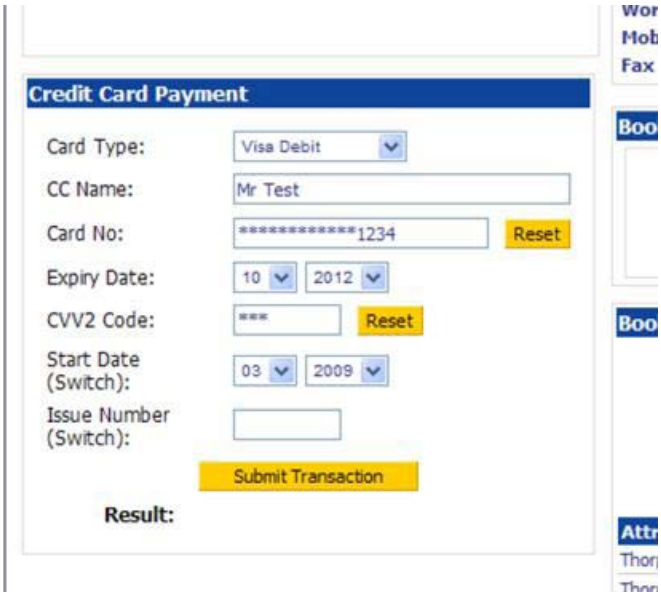

Figure 9 - A series of **** show entry progress

Once all the required information has been entered the payment server processes the card and returns an authorisation code back to the CIM script. The contact centre agent never hears (or sees) any of the credit card details.

By using a telephony platform that is itself located outside of the company premises (i.e. within the telephony cloud) it is possible for a company to dramatically reduce their PCI compliance commitments as no credit card information enters the premises.

Conclusion

All contact centres that take credit card payments must ensure that they meet the 12 Payment Card Industry Data Security Standard (PCI DSS) requirements. Implementing such requirements can be a complex, time consuming and expensive task. CIM systems can effectively be used to help companies comply with these requirements.

PCI DSS requirements 3 and 4 cover protecting cardholder data. This is achieved by ensuring that stored card information is encrypted at all times and that sensitive data is deleted the moment it is no longer required. A modern CIM system will allow fields to be encrypted and have mechanisms to ensure that the encrypted data can be sent securely to third parties for processing. Maintenance tools should be available to securely remove encrypted data automatically once the card details have been processed.

Ideally, no credit card data should be stored within company databases (even in an encrypted format). Additionally credit card information can find its way into other systems such as email mailboxes and call recording files. CIM systems offer a range of payment gateways to address this problem. These enable transactions to be processed in real time thereby negating the need to store such information or send emails with encrypted file attachments.
Use of computer telephony interfaces (CTI) allows the CIM system to instruct the contact centre's call recording system to pause recording whilst the credit card details are being taken thereby ensuring that no sensitive data is stored within the produced audio files.

The biggest advantage of CIM scripted solutions from a PCI compliance viewpoint is that they offer the opportunity for a company to totally remove their PCI DSS obligations by ensuring that no credit card information enters the company's premises. This is achieved by using a CIM interface to remotely control a network hosted telephony platform and take credit card information via a series of DTMF tones entered by the caller on their telephone keypad.

The author

Geoff Forsyth BEng, CEng, MBCS, CITP, FRSA, is the founding Chief Technical Officer of IPPlus Plc, a British AIM listed company based in Ipswich, Suffolk. The company runs three distinct divisions: CallScripter, a software company producing integrated applications for the contact centre industry; Ansaback, a 24/7 bureau contact centre operation and IP3 Telecom, a network solution provider.

Over the past decade Geoff has advised on specification, project management, configuration and maintenance of both traditional ISDN and state of the art VoIP technologies. Geoff's technical knowledge and know how ensures that this 'thought leader' is well placed to provide an insightful look into the current and future trends of the modern contact centre.

Geoff is a Chartered IT Professional through the British Computer Society and a Fellow of the RSA.

The company

CallScripter is the next generation scripting tool, designed to maximise contact centre productivity whilst improving both agent and business efficiency.

CallScripter has rightfully gained a reputation as a best of breed CIM software supplier both in the UK and internationally.

CallScripter's background comes from not only producing software but also running a 100 seat 24/7, 365 days a year commercial contact centre. The resulting wealth of knowledge and hands-on experience obtained enables CallScripter to provide relevant 'real world' effective scripting software. Having a sizable contact centre in-house drives forward technological advances and best practice procedures.

CallScripter software solution is fast and flexible and can create the most sophisticated call scripts. Facilitating the rapid set-up, handling and reporting of campaigns, CallScripter's open architecture allows for easy integration into third party applications. The product is available in both a premise and hosted (SaaS) environment.

CallScripter
2 Melford Court, The Havens,
Ransomes Europark
Ipswich, Suffolk UK IP3 9SJ
Telephone/Fax 0800 088 7470
www.callscripter.com

CallScripter